

04-04-02

2131

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE**INFORMATION DISCLOSURE
STATEMENT**Docket Number:
10746/31Application Number
10/080,647Filing Date
February 22, 2002Examiner
Not Yet AssignedArt Unit
2131Title
**DISTRIBUTED DIGITAL SIGNATURE
GENERATION METHOD AND DIGITALLY
SIGNED DIGITAL DOCUMENT GENERATION
METHOD AND APPARATUS**Applicant(s)
HORITA, et al.**RECEIVED****APR 09 2002**Address to:
Assistant Commissioner for Patents
Washington, D.C. 23201**Technology Center 2100**

1. In accordance with the duty of disclosure under 37 C.F.R. § 1.56 and in conformance with the procedures of 37 C.F.R. §§ 1.97 and 1.98 and M.P.E.P. § 609, attorney(s) for Applicant(s) hereby bring the reference(s) listed on the attached modified PTO Form No. 1449 to the attention of the Examiner. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the reference(s) be made of record therein and appear among the "References Cited" on any patent to issue therefrom.
2. A copy of each patent, publication or other information listed on the modified PTO form 1449 is enclosed, except as otherwise indicated.

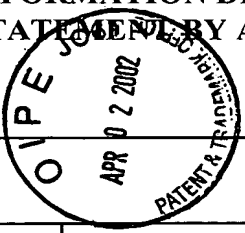
Dated: 4/2/2002By: 

Aaron C. Deditch (Reg. No. 33,865)

KENYON & KENYON
One Broadway
New York, N.Y. 10004
(212) 425-7200 (telephone)
(212) 425-5288 (facsimile)**CUSTOMER NO. 26646**

EXPRESS MAIL LABEL NO.: EV 003628470 US

| | | |
|--|----------------------------------|-------------------------------|
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT | ATTY. DOCKET NO. 10746/31 | U.S. SERIAL NO. 10/080,647 |
| | APPLICANT(S) HORITA et al. | |
| | FILING DATE February 22, 2002 | GROUP 2131 |



U. S. PATENT DOCUMENTS

| EXAMINER INITIAL | PATENT NUMBER | PATENT DATE | NAME | CLASS | SUBCLASS | FILING DATE* |
|---------------------|------------------|----------------|------------------|-------|----------|-----------------|
| | 5,625,692 | April 29, 1997 | HERZBERG, et al. | | | |
| | | | | | | |

FOREIGN PATENT DOCUMENTS

| EXAMINER INITIAL | DOCUMENT NUMBER | DATE | COUNTRY | CLASS | SUBCLASS | TRANSLATION | |
|---------------------|--------------------|--------------------|---------|-------|----------|-------------|----|
| | | | | | | YES | NO |
| | 8-251157 | September 27, 1996 | Japan | | | * | |
| | 9-205422 | August 5, 1997 | Japan | | | | |

*Corresponds to U.S. Patent No. 5,625,692, also enclosed.

**Description corresponds to that of 8-251157.

APR 09 2002
Technology Center 2100

OTHER DOCUMENTS

| EXAMINER INITIAL | AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC. |
|---------------------|--|
| | BONEH, D., and FRANKLIN, M., "Efficient Generation of Shared RSA Keys", Proceedings of Crypto, 1997, pp. 425-439. |
| | WU, et al., "Building Intrusion Tolerant Applications", Proceedings of 8 th UNENIX Security Symposium, USENIX, 1999. |
| | SHAMIR, A., "How to Share a Secret", Communications of ACM, Vol. 22, pp.612-613, 1979. |
| | MIYAZAKI, SAKURAI, MOGI, "On Distributed Cryptographic Protocol for Threshold RSA Signing and Decrypting with No Dealer", IEICE Transactions Fundamentals, Vol. E84-A, No. 5, May 2001, pp. 1177-1183. |
| | RIVEST, R.L., SHAMIR, A., ADLEMAN, L., "A Method for Obtaining Digital Signature and Public Key Cryptosystems", Communications of ACM, Vol. 21, pp. 1-15, 1978. |
| | SHOUP, V., "Practical Threshold Signatures", Proceedings of Eurocrypt '2000, 2000. |
| | |

| | |
|---|-----------------|
| EXAMINER | DATE CONSIDERED |
| EXAMINER: Initial if citation considered, whether or not citation is in conformance with M.P.E.P. 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. | |